

CLAIM AMENDMENTS

1.(Currently amended) A method for biometrically securing access to ~~an electronic system~~, said method comprising the steps of:

wirelessly obtaining identification of a user with an electronic system using a contactless card reader in communication with said electronic system, the identification of said user further retrieved from a contactless smart card after said contactless smart card establishes a contactless link to support wireless communication between said contactless smart card and said contactless card reader ~~presented to the electronic system by said user;~~

accessing a user profile including biometric attributes associated with said user through a computer network from a remote server based on the identification of said user obtained wirelessly from said contactless smart card;

prompting said user to input to a biometric user interface associated with said electronic system at least one biometric attribute randomly selected from said user profile ~~retrieved from said remote server containing biometric attributes of said user; and~~

said electronic system permitting said user access to perform a user-desired activity with the electronic system if at least one biometric attribute input by said user to said biometric user interface associated with said electronic system matches said at least one biometric attribute randomly selected from said user profile.

2.(Previously presented) The method of claim 1 wherein said computer network is a secure computer network.

3.(Currently amended) The method of claim 1 wherein said remote server is user profile is ~~stored in~~ a biometric broker.

4.(Previously presented) The method of claim 1 further comprising the steps of:

obtaining at least one biometric attribute from said user for compilation in said user profile; compiling said user profile; and

storing said user profile in said server accessible by at least one biometric user interface associated with said electronic system.

5.(Original) The method of claim 4 further comprising the step of:

permitting said user to modify said user profile, in response to approval of a request by said user.

6.(Canceled).

7.(Currently amended) The method of claim [6] 1 further comprising the step of:

subsequently prompting a user to input to said biometric user interface associated with said electronic system at least one additional biometric attribute randomly selected from said user profile, if at least one biometric attribute previously input by said user to said biometric user interface associated with said electronic system does not match said at least one biometric attribute previously randomly selected from said user profile.

8.(Original) The method of claim 1 wherein said electronic system comprises at least one wireless device that operates with a wireless network.

9.(Original) The method of claim 1 wherein said electronic system comprises at least one computer workstation operable over an associated network.

10.(Original) The method of claim 1 wherein said electronic system comprises an automated teller machine.

11.(Currently amended) The method of claim 1 wherein said electronic system comprises a secured entry system to a secured environment.

12.(Original) The method of claim 1 wherein said electronic system comprises a wireless network.

13. (Canceled)

14.(Original) The method of claim 1 wherein said electronic system comprises a wireless device.

15.(Previously presented) The method of claim 1 further comprising the steps of:

identifying at least one defective biometric attribute associated with said user; and thereafter prompting a user to input to said biometric user interface associated with said electronic system at least one additional biometric attribute randomly selected from said user profile containing biometric attributes of said user.

16.(Original) The method of claim 1 wherein said user-desired activity comprises a financial transaction.

17.(Original) The method of claim 1 wherein said user-desired activity comprises an ATM transaction.

18.(Original) The method of claim 1 wherein said user-desired activity comprises access to a secure area.

19.(Original) The method of claim 1 wherein said user-desired activity comprises access to data from said electronic system.

20.(Original) The method of claim 1 wherein said user-desired activity comprises execution of a mechanical activity.

21.(Original) The method of claim 1 further comprising the step of:

initiating access to said electronic system utilizing only one biometric attribute input to said electronic system.

22.(Currently amended) A method for biometrically securing access to a secure area ~~an electronic system~~, said method comprising the steps of:

wirelessly obtaining identification of a user by an electronic system using a contactless card reader in communication with said electronic system, the identification of said user further retrieved from a contactless smart card after said contactless smart card establishes a contactless link with said contactless card reader that supports wireless communication between said contactless smart card and said contactless card reader—presented to the electronic system by said user;

based on said wirelessly obtained identification, said electronic system using a computer network to obtain a user profile associated with said user from a remote server said user profile including biometric attributes;

said electronic system prompting [a] said user to input into a biometric user interface associated with said electronic system at least [two] one biometric attribute ~~attributes~~ randomly selected by said electronic system from said user profile retrieved from said remote server containing biometric attributes of said user; and

permitting said user to access a secure area ~~perform a user desired activity at said electronic system if~~ said at least one biometric attribute ~~attributes~~ input by said user to said biometric user interface match biometric attributes included in said user profile in an order that said at least one biometric attribute is requested by associated with said electronic system matches said at least two biometric attributes randomly selected from said user profile.

23.(Currently amended) A system for biometrically securing access ~~to an electronic system,~~ said system comprising:

an electronic system adapted to permit a user to perform a user-desired activity if at least one biometric attribute input by the user to said biometric user interface matches said at least one biometric attribute randomly selected from a user profile accessible by the electronic system from a remote server based on identification of a user obtained wirelessly from a contactless smart card presented to in wireless communication with a contactless card reader associated with the electronic system by the user, wherein said smart card is adapted to store at least one user profile including biometric attributes and provide said electronic system access to said at least one user profile;

a contactless smart card reader associated with said electronic system; and

a biometric user interface associated with said electronic system adapted to enable said user to input at least one biometric to said electronic system for comparison to at least one biometric attribute randomly selected by said electronic system from said user profile;

wherein said electronic system is adapted to permit said user to perform a user-desired activity[,] if at least one biometric attribute input by said user to said biometric user interface matches said at least one biometric attribute randomly selected from said user profile by said electronic system.

24.(Cancelled).

25.(Previously presented) The system of claim 23 wherein said user profile is accessible from a biometric broker via a secure network connection.

26.(Previously presented) The system of claim 23 wherein: at least one biometric attribute is obtained from said user for compilation in said user profile.

27.(Previously presented) The system of claim 23 wherein said user is permitted to modify said user profile, in response to approval of a request by said user.

28.(Previously presented) The system of claim 23 further comprising:

module for comparing at least one biometric attribute input by said user to said biometric user interface associated with said electronic system with said at least one biometric attribute randomly selected from said user profile.

29.(Previously presented) The system of claim 28 further comprising:

module for subsequently prompting said user to input to said biometric user interface associated with said electronic system at least one additional biometric attribute randomly selected from said user profile, if at least one biometric attribute previously input by said user to said biometric user interface associated with said electronic system does not match said at least one biometric attribute randomly previously selected from said user profile.

30.(Original) The system of claim 23 wherein said electronic system comprises at least one wireless device that operates with a wireless network.

31.(Currently amended) The system of claim 23 wherein said electronic system comprises at least one computer workstation accessible over said computer network.

32.(Original) The system of claim 23 wherein said electronic system comprises an automated teller machine.

33.(Original) The system of claim 23 wherein said electronic system comprises a secured entry system to a secured environment.

34.(Previously amended) The system of claim 23 wherein said computer network comprises a wireless network.

35.(Cancelled).

36.(Original) The system of claim 23 wherein said electronic system comprises a wireless device.

37.(Previously presented) The system of claim 23 further comprising:

module for identifying at least one defective biometric attribute associated with said user; and

wherein said user is thereafter prompted to input to said electronic system at least one additional biometric attribute randomly selected from a user profile containing biometric attributes of said user.

38.(Original) The system of claim 23 wherein said user-desired activity comprises a financial transaction.

39.(Original) The system of claim 23 wherein said user-desired activity comprises an ATM transaction.

40.(Original) The system of claim 23 wherein said user-desired activity comprises access to a secure area.

41.(Original) The system of claim 23 wherein said user-desired activity comprises access to data from said electronic system.

42.(Original) The system of claim 23 wherein said user-desired activity comprises execution of a mechanical activity.

43. (Original) The system of claim 23 wherein access to said electronic system is initiated utilizing only one biometric attribute input to said electronic system.

44.(Currently amended) A system for biometrically securing access to a secure area ~~an electronic system~~, said system comprising:

an electronic system including a contactless smart card reader, a biometric interface and access over a computer network to a remote server, said electronic system adapted to permit a user to access a secure area perform a user-desired activity if at least one biometric attribute input by the user to said biometric user interface matches ~~said~~ at least one biometric attribute randomly selected by said electronic system from ~~said~~ a user profile accessible by the electronic system over [a] said computer network from [a] said remote server, said ~~electronic system including access to a remote server through electronic connection to a computer network, and said~~ remote server adapted to store at least one user profile including biometric attributes and provide said electronic system access to said at least one user profile and said electronic system further adapted to wireless retrieve user identification from a contactless

smart card through said contactless smart card reader after a wireless communication link is established between said contactless smart card reader and a contactless smart card held by the user;

~~a smart card reader associated with said electronic system; and~~

~~a biometric user interface associated with said electronic system adapted to enable said user to input at least one biometric to said biometric user interface for comparison to at least two biometric attributes randomly selected by said electronic system from said user profile;~~

~~wherein said electronic system is adapted to permit said user to perform a user desired activity, if at least one biometric attribute input by said user to said biometric user interface matches said at least one biometric attribute randomly selected from said user profile by said electronic system.~~